Enterprise Data Security for Microsoft Entra ID

As the backbone of identity and access management (IAM) for Microsoft Cloud resources, Entra ID (formerly Azure Active Directory) is crucial for maintaining business continuity. Identity resilience starts with behavioral insights — Druva's fully managed solution provides a simple, efficient, and automated way to protect and recover Microsoft Entra ID objects, ensuring your organization remains resilient.

The Challenge

Microsoft Entra data shows attempted password attacks increased more than tenfold in 2023, from around 3 billion per month to over 30 billion. This translates to an average of 4,000 attempted attacks per second targeting Microsoft Cloud identities[1]. If Entra ID isn't available, your users can't work in Microsoft 365 or Azure Cloud. To ensure resilience against Entra ID outages, compromises, and misconfigurations, your organization must have reliable access to its data.

The Solution

Druva Identity Resilience for Microsoft Entra ID enables organizations to take a policy-driven approach to protect their Azure Identity and Access Management, minimizing downtime and expediting the recovery of critical data and services.

Druva's fully managed SaaS Solution provides a simple and efficient way to ensure you can recover your Microsoft Entra ID objects quickly, avoiding costly disruptions and reputational damage to your organization. By storing data in logically air-gapped storage fully hosted by Druva, you ensure your Entra ID directory services are immutable and can be restored efficiently in the event of cyber threats, data loss, misconfiguration, or accidental deletion.

Customer Benefits

- Maintain Business Continuity for Microsoft 365 & Azure: Keep users productive by enabling recovery of critical Entra ID objects when Entra ID is unavailable or disrupted.
- **Reduce Downtime with Policy-Driven Recovery:** Minimize downtime and expedite recovery of critical identity data and services.
- **Recover Function, Not Just Objects:** Restore objects with their settings and relationships to preserve access integrity (for example, group memberships).
- **Increase Security Readiness:** Layered security and built-in intelligence for early threat detection, supporting faster incident response and remediation.

Use Cases

- **Cyber Recovery (Threats, Compromise):** Restore Entra ID directory services efficiently from logically air-gapped, immutable backups after cyber threats or compromise.
- **Operational Recovery (Misconfiguration, Accidental Deletion):** Recover Entra ID objects quickly after misconfiguration or accidental deletion to reduce disruption and reputational impact.
- **Identity Resilience During Entra ID Unavailability:** Ensure reliable access to identity data to preserve user access to Microsoft 365 and Azure Cloud services.
- **Governance & Portability Workflows:** View/download device metadata for governance needs and export/import backed-up Entra ID data (JSON export; PowerShell import to a new Entra ID instance).
- **Hybrid IdP Environment Protection:** Whether you use Entra ID for cloud resources, Okta for SSO, or legacy AD for on-premises infrastructure, Druva provides a single pane of glass to manage protection for all three.

[1] Microsoft Digital Defense Report 2023

© Copyright 2026 | Druva Inc. | druva.com

Key Features

Druva Offers Comprehensive Protection for Entra ID Objects (Including Settings & Relationships)

- **Users & Relationships** — Get a policy-based approach to automatically protect user objects and their associated metadata. Restore users along with their relationships, such as organizational hierarchy and reporting structures, ensuring continuity.
- **Groups & Memberships** — Safeguard group objects and maintain the integrity of group memberships. Recover groups with their exact member lists intact, crucial for maintaining access controls and operational workflows.
- **Roles & Associations** — Protect role objects and their associations with users and groups. Ensure that role-based access controls are quickly restored, maintaining security and compliance post-recovery.
- **Devices (View / Download Only)** — Back up device metadata and configurations. View and download device information to facilitate governance and compliance requirements.
- **Export & Import Backed-Up Data** — Export the backed-up Entra ID as a JSON file and import it into a new Entra ID instance via PowerShell.
- **Enterprise Applications** — Protect enterprise applications by backing up application objects and their settings. Recover enterprise applications to their configured states, including permissions and connected services.
- **App Registrations** — Secure application registration details, including client IDs. Restore app registrations with exact configurations, preserving essential integrations and access privileges across applications.
- **Administrative Units** — Protect administrative unit objects with their properties, memberships, and delegated roles, ensuring organizational structure and scoped administration are preserved.
- **Conditional Access Policies** — Safeguard conditional access objects with their properties, assignments, and access controls, enabling seamless restoration of security policies and enforcement rules.
- **Protect Microsoft Entra PIM Settings** — Back up Privileged Identity Management (PIM) configurations, ensuring that high-risk administrative access rules are secure. Get point-in-time restore to previous snapshots and export settings for governance and portability.

Why Druva?

With Druva, businesses can quickly restore Entra ID services, ensuring continuity and resilience against cyber threats and misconfigurations. Druva is among the first in the industry to meet this demand, filling a customer need, and addressing core IAM needs. Overall, the addition of Entra ID support strengthens Druva's comprehensive data protection suite for Identity and Microsoft environments, enhancing user experience, operational efficiency, and market competitiveness.

Visit druva.com/solutions/microsoft-entra-id to learn more.

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by nearly 7,500 customers, including 75 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world. Visit druva.com and follow us on LinkedIn, X (formerly Twitter), and Facebook.

© Copyright 2026 | Druva Inc. | druva.com